

Entanglement purification with noisy apparatus can be used to factor out an eavesdropper

Hans Aschauer* and Hans J. Briegel†

*Section Physik, Ludwig-Maximilians-Universität,
Theresienstr. 37, D-80333 München, Germany*

(Dated: January 29, 2002)

We give a proof that entanglement purification, even with noisy apparatus, is sufficient to disentangle an eavesdropper (Eve) from the communication channel. Our proof applies to all possible attacks (individual and coherent). Due to the quantum nature of the entanglement purification protocol, it is also possible to use the obtained quantum channel for secure transmission of quantum information.

I. INTRODUCTION

Quantum communication exploits the quantum properties of its information carriers for communication purposes such as the distribution of secure cryptographic keys in quantum cryptography [1, 2] and the communication between distant quantum computers in a network [3]. A central problem of quantum communication is how to faithfully transmit unknown quantum states through a noisy quantum channel [4]. While information is sent through such a channel (for example an optical fiber), the carriers of the information interact with the channel, which gives rise to the phenomenon of decoherence and absorption; an initially pure quantum state becomes a mixed state when it leaves the channel. For quantum communication purposes, it is however necessary that the transmitted qubits retain their genuine quantum properties, for example in form of an entanglement with qubits on the other side of the channel.

In quantum cryptography, noise in the communication channel plays a crucial role: In the worst-case scenario, all noise in the channel is attributed to an eavesdropper, who manipulates the qubits in order to gain as much information on their state as possible, while introducing only a moderate level of noise.

To deal with this situation, two different techniques have been developed: *Classical privacy amplification* allows the eavesdropper to have partial knowledge about the raw key built up between the communicating parties Alice and Bob. From the raw key, a shorter key is “distilled” about which Eve has vanishing (i.e. exponentially small in some chosen security parameter) knowledge. Despite of the simple idea, proofs taking into account all eavesdropping attacks allowed by the laws of quantum mechanics have shown to be technically involved [5, 6, 7]. Recently, Shor and Preskill [8] have given a simpler physical proof relating the ideas in [5, 6] to quantum error correcting codes [9] and, equivalently, to one-way entanglement purification protocols. *Quantum privacy amplification* (QPA) [10], on the other hand, employs a two-way entanglement purification recurrence protocol [11] that

*Electronic address: Hans.Aschauer@Physik.uni-muenchen.de

†Electronic address: Hans.Briegel@Physik.uni-muenchen.de

eliminates any entanglement with an eavesdropper by creating a few perfect EPR pairs out of many imperfect (or impure) EPR pairs. The perfect EPR pairs can then be used for secure key distribution in entanglement-based quantum cryptography [2, 10, 12]. In principle, this method guarantees security against any eavesdropping attack. However, the problem is that the QPA protocol assumes ideal quantum operations. In reality, these operations are themselves subject to noise. As shown in [13, 14, 15], there is an upper bound F_{\max} for the achievable fidelity of EPR pairs which can be distilled using noisy apparatus. *A priori*, there is no way to be sure that there is no residual entanglement with an eavesdropper. This problem could be solved if Alice and Bob had fault tolerant quantum computers at their disposal, which could then be used to reduce the noise of the apparatus to any desired level. This was an essential assumption in the security proof given by Lo and Chau [16].

In this paper, we show that the standard two-way entanglement purification protocols alone, which have been developed by Bennett *et al.* [11, 17] and later by Deutsch *et al.* [10], with some minor modifications to accomodate certain security aspects as discussed below, can be used to efficiently establish a *perfectly private quantum channel*, even when both the physical channel connecting the parties and the local apparatus used by Alice and Bob are noisy.

In Section II we will briefly review the concepts of entanglement purification. Section III will give the main result of our work: we prove that it is possible to *factor out* an eavesdropper using EPP, even when the apparatus used by Alice and Bob is noisy. We conclude the paper with a discussion in Section IV.

II. ENTANGLEMENT PURIFICATION

As two-way entanglement purification protocols (2-EPP) play an important role in this paper, we will briefly review one example of a recurrence protocol which was described in [10], and called *quantum privacy amplification* (QPA) by the authors. It is important to note that we distinguish the entanglement purification *protocol* from the distillation *process*: the first consists of probabilistic local operations (unitary rotations and measurements), where two pairs of qubits are combined, and either one or zero pairs are kept, depending on the measurement outcomes. The latter, on the other hand, is the procedure where the purification protocol is applied to large ensemble of pairs recursively (see Fig. (1)).

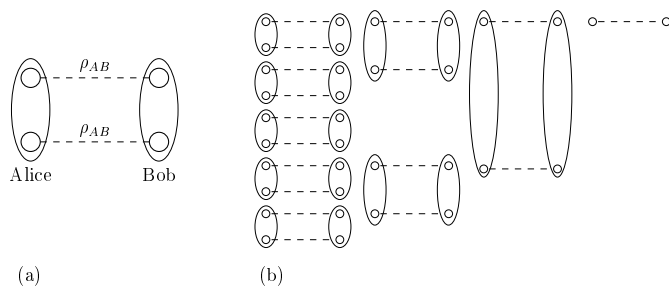


FIG. 1: The entanglement purification protocol (a) and the entanglement distillation process (b).

In the quantum privacy amplification 2-EPP, two pairs of qubits, shared by Alice and Bob, are considered to be in the state $\rho_{A_1 B_1} \otimes \rho_{A_2 B_2}$. Without loss of generality (see later),

we may assume that the state of the pairs is of the Bell-diagonal form,

$$\rho_{AB} = A |\Phi^+\rangle\langle\Phi^+| + B |\Psi^-\rangle\langle\Psi^-| + C |\Psi^+\rangle\langle\Psi^+| + D |\Phi^-\rangle\langle\Phi^-|. \quad (1)$$

Following [10], the protocol consists of three steps:

1. Alice applies to her qubits a $\pi/2$ rotation, U_x , Bob a $-\pi/2$ rotation about the x axis, U_x^{-1} .
2. Alice and Bob perform the bi-lateral CNOT operation

$$\text{BCNOT}_{A_1B_1}^{A_2B_2} = \text{CNOT}_{A_1}^{A_2} \otimes \text{CNOT}_{B_1}^{B_2}$$

on the four qubits.

3. Alice and Bob measure both qubits of the target pair A_2B_2 of the BCNOT operation in the z direction. If the measurement results coincide, the source pair A_1B_1 is kept, otherwise it is discarded. The target pair is always discarded, as it is projected onto a product state by the bilateal measurement.

By a straightforward calculation, one gets the result that the state of the remaining pair is still a Bell diagonal state, with the diagonal coefficients [10]

$$\begin{aligned} A' &= \frac{A^2 + B^2}{N}, & B' &= \frac{2CD}{N} \\ C' &= \frac{C^2 + D^2}{N}, & D' &= \frac{2AB}{N}, \end{aligned} \quad (2)$$

and the normalization coefficient $N = (A + B)^2 + (C + D)^2$, which is the probability that Alice's and Bob's measurement results in step 3 coincide. Note that, up to the normalization, these recurrence relations are a quadratic form in the coefficients A, B, C , and D . These relations allow for the following interpretation (which can be used to obtain the relations (2) in the first place): As all pairs are in the Bell diagonal state (1), one can interpret A, B, C , and D as the relative frequencies in the ensemble of all pairs of the states $|\Phi^+\rangle, |\Psi^-\rangle, |\Psi^+\rangle$, and $|\Phi^-\rangle$, respectively. By looking at (2) one finds that the result of combining two $|\Phi^+\rangle$ or two $|\Psi^-\rangle$ pairs is a $|\Phi^+\rangle$ pair, combining a $|\Psi^+\rangle$ and a $|\Phi^-\rangle$ (or vice versa) yields a $|\Psi^-\rangle$ pair, and so on. Combinations of A, B, C , and D that do not occur in (2), namely AC, AD, BC and BD , are “filtered out”, i.e. they give different measurement results for the bilateral measurement in step 3 of the protocol. We will use this way of calculating recurrence relations for more complicated situations later.

Numerical calculations [10] and, later, an analytical investigation [18] have shown that for all initial states (1) with $A > 1/2$, the recurrence relations (2) approach the fixpoint $A = 1, B = C = D = 0$; this means that given a sufficiently large number of initial pairs, Alice and Bob can distill asymptotically pure EPR pairs.

III. FACTORIZATION OF EVE

In the previous section it has been assumed that Alice and Bob have perfect apparatus at their disposal, which they use to execute the protocol. For the following security analysis, we

shall consider a more general scenario where this assumption is abandoned. As mentioned in the introduction, there is an upper bound F_{\max} for the attainable fidelity of the distilled pairs, when the apparatus used by Alice and Bob is noisy [13, 14]. For quantum cryptography the question arises: can these imperfect pairs still be used for secure key distribution?

In this section we will show that 2-EPP with noisy apparatus is sufficient to factor out Eve in the Hilbertspace of Alice, Bob, their labs and Eve. For the proof, we will first introduce the concept of the lab demon as a simple model of noise. Then we will consider the special case of binary pairs, where we have obtained analytical results. Using the same techniques, we generalize the result to the case of Bell diagonal ensembles. The most general case of correlated non Bell-diagonal can be reduced to the case of Bell diagonal states [19].

A. The effect of noise

In this section we will answer the following question: what is the effect of an error, introduced by some noisy operation at a given point of the distillation process? To keep the argument transparent, we restrict our attention to the following type of noise:

- It acts locally, i.e. noise does not introduce correlations between remote quantum systems.
- Noise is memoryless, i.e. on a timescale imposed by the sequence of steps in a given protocol, there are no correlations between the “errors” that occur at different times.

The action of noisy apparatus on a quantum system in state $\rho \in \mathcal{B}(\mathcal{H})$ can be formally described by some trace conserving, completely positive map. Any such map can be written in the operator-sum representation [4, 20],

$$\rho \rightarrow \sum_i A_i \rho A_i^\dagger, \quad (3)$$

with linear operators A_i , that fulfill the normalization condition $\sum_i A A^\dagger = \mathbf{1}$. The operators A_i are the so-called *Kraus operators* [20].

As we have seen above, in the purification protocol the CNOT operation, which acts on two qubits a and b , plays an important role. For that reason, it is necessary to consider noise which acts on a two-qubit Hilbert space $\mathcal{H} = \mathbb{C}_a^2 \otimes \mathbb{C}_b^2$. Eq. (3) describes the most general non-selective operation that can, in principle, be implemented. For technical reasons, however, we restrict our attention to the case that the Kraus operators are proportional to products of Pauli matrices. The reason for this choice is that Pauli operators map Bell states onto Bell states, which will allow us to introduce the very useful concept of *error flags* later. Eq. (3) can then be written as

$$\rho_{ab} \rightarrow \sum_{\mu, \nu=0}^3 f_{\mu\nu} \sigma_\mu^{(a)} \sigma_\nu^{(b)} \rho_{ab} \sigma_\mu^{(a)} \sigma_\nu^{(b)}, \quad (4)$$

with the normalization condition $\sum_{\mu, \nu=0}^3 f_{\mu\nu} = 1$. Note that Eq. (4) includes, for an appropriate choice of the coefficients $f_{\mu\nu}$, the one- and two-qubit depolarizing channel and combinations thereof, as studied in [13, 14]; but it is more general. Below, we will refer to these special Kraus operators as *error operators*.

The coefficients $f_{\mu\nu}$ can be interpreted as the joint probability that the Pauli rotations σ_μ and σ_ν occur on qubits a and b , respectively. For pedagogic purposes we employ the following interpretation of (4): Imagine that there is a (fictitious) little demon in Alice's laboratory – the “lab demon” – which applies in each step of the distillation process randomly, according to the probability distribution $f_{\mu\nu}$, the Pauli rotation σ_μ and σ_ν to the qubits a and b , respectively. The lab demon summarizes all relevant aspects of the lab degrees of freedom involved in the noise process.

Noise in Bob's laboratory, can, as long as we restrict ourselves to Bell diagonal ensembles, be attributed to noise introduced by Alice's lab demon, without loss of generality. It is also possible to think of a second lab demon in Bob's lab who acts similarly to Alice's lab demon. This would, however, not affect the arguments employed in this paper.

The lab demon does not only apply rotations randomly, he also maintains a list in which he keeps track of which rotation he has applied to which qubit pair in which step of the distillation process. What we will show in the following section is that, from the mere content of this list, the lab demon will be able to extract – in the asymptotic limit – full information about the state of each residual pair of the ensemble. This will then imply that, given the lab demon's knowledge about the flags, the state of the distilled ensemble is a tensor product of pure Bell states. Eve cannot not have information on the specific sequence of Bell pairs (in addition to their relative frequencies) — otherwise she would also be able to learn, to some extent, at which stage the lab demon has applied which rotation.

From that it follows that Eve is factored out, i. e. Alice and Bob describe their pairs with the state

$$\rho_{\text{ABEL}} = \left(\sum_{i,j=0}^1 f_{\text{L}}^{(i,j)} |\mathcal{B}_{i,j}\rangle_{\text{AB}} \langle \mathcal{B}_{i,j}| \right) \otimes \rho_{\text{E}}. \quad (5)$$

It remains to be shown that the same argument applies to a realistic scenario where the lab demon is replaced by some “real” noise source. To be specific, in the following argument we show that *all* quantum or classical devices that share the same noise characteristics are equally secure. First we note that a communication protocol is secure if and only if there exists no eavesdropping strategy; this fact can, in principle, be determined by cooperating communication parties. On the other hand, all devices with identical noise characteristics are quantum mechanically described by the same completely positive trace conserving map, so that a initial state ρ_i is mapped onto a final state ρ_f , independent from the physical realization of the map. This means that there is no way to distinguish the devices by only looking at the input and output states. For the case of noisy apparatus that is used for entanglement purification we get thus the following result: a device that implements (4) with a lab demon cannot be distinguished from any device that introduces noise due to some “real” noise source; in particular, the devices must lead to the same level of security (regardless whether or not error flags are measured or calculated by anybody): otherwise they would be distinguishable.

In order to separate conceptual from technical considerations and to obtain analytical results, we will first concentrate on the special case of binary pairs and a simplified error model. After that, we generalize the results to ensembles which are diagonal in the Bell basis.

B. Binary pairs

In this section we restrict our attention to pairs in the state

$$\rho_{AB} = A |\Phi^+\rangle_{AB} \langle \Phi^+| + B |\Psi^+\rangle_{AB} \langle \Psi^+|, \quad (6)$$

and to errors of the form

$$\rho_{AB}^{(1)} \otimes \rho_{AB}^{(2)} \rightarrow \sum_{\mu, \nu \in \{0,1\}} f_{\mu\nu} U_\mu^{(1)} U_\nu^{(2)} \rho_{AB}^{(1)} \otimes \rho_{AB}^{(2)} U_\mu^{(1)\dagger} U_\nu^{(2)\dagger} \quad (7)$$

with $U_0^{(1,2)} = \text{id}^{(1,2)}$ and $U_1^{(1,2)} = \sigma_x^{(1,2)}$. Eq. (7) describes a *two-bit correlated spin-flip channel*. The indices 1 and 2 indicate the source and target bit of the bilateral CNOT (BCNOT) operation, respectively. It is straightforward to show that, using this error model in the 2-EPP, binary pairs will be mapped onto binary pairs.

At the beginning of the distillation process, Alice and Bob share an ensemble of pairs described by (6). Let us imagine that the lab demon attaches one classical bit to each pair, which he will use for book-keeping purposes. At this stage, all of these bits, which we call “error flags”, are set to zero. This reflects the fact that the lab demon has the same *a priori* knowledge about the state of the ensemble as Alice and Bob.

In each purification step, two of the pairs are combined. The lab demon first simulates the noise channel (7) on each pair of pairs by the process described. Whenever he applies a σ_x operation to a qubit, he inverts the error flag of the corresponding pair. Alice and Bob then apply the 2-EPP to each pair of pairs; if the measurement results in the last step of the protocol coincide, the source pair will be kept. Obviously, the error flag of that remaining pair will also depend on the error flag of the target pair, i.e. the error flag of the remaining pair is a function of the error flags of both “parent” pairs, which we call the *flag update function*. Since for binary pairs the error flag consists of one bit, there are 16 different flag update functions in total. From these, the lab demon chooses the logical AND function as the flag update function, i.e. the error flag of the remaining pair is set to “1” if and only if both parent’s error flags had the value “1”.

After each purification step, the lab demon divides all pairs into two subensembles, according to the value of their error flags. By a straightforward calculation, one finds for the coefficients A_i and B_i , which completely describe the state of the pairs in the subensemble i , the following recurrence relations:

$$\begin{aligned} A'_0 &= \frac{1}{N} (f_{00}(A_0^2 + 2A_0A_1) + f_{11}(B_1^2 + 2B_0B_1) \\ &\quad + f_s(A_0B_1 + A_1B_1 + A_0B_0)) \\ A'_1 &= \frac{1}{N} (f_{00}A_1^2 + f_{11}B_0^2 + f_sA_1B_0) \\ B'_0 &= \frac{1}{N} (f_{00}(B_0^2 + 2B_0B_1) + f_{11}(A_1^2 + 2A_0A_1) \\ &\quad + f_s(B_0A_1 + B_1A_1 + B_0A_0)) \\ B'_1 &= \frac{1}{N} (f_{00}B_1^2 + f_{11}A_0^2 + f_sB_1A_0) \end{aligned} \quad (8)$$

with $N = (f_{00} + f_{11})((A_0 + A_1)^2 + (B_0 + B_1)^2) + 2f_s(A_0 + A_1)(B_0 + B_1)$ and $f_s = f_{01} + f_{10}$.

For the case of uncorrelated noise, $f_{\mu\nu} = f_\mu f_\nu$, we find an analytical expression for the relevant fixpoint of the map (8):

$$\begin{aligned} A_0^\infty &= \frac{4f_0^2 - 4f_0 + (2f_0 - 1)\sqrt{4f_0 - 3} + 1}{2(2f_0 - 1)^2}, \\ A_1^\infty &= 0, \quad B_0^\infty = 0, \quad B_1^\infty = 1 - A_0^\infty. \end{aligned} \quad (9)$$

Note that, while Eq. (9) gives a fixpoint of (8) for $f_0 \geq 3/4$, this does not imply that this fixpoint is an attractor. In order to investigate the attractor properties, we calculate the eigenvalues of the matrix of first derivatives,

$$M_D = \left(\begin{array}{ccc} \frac{\partial A'_0}{\partial A_0} & \cdots & \frac{\partial B'_1}{\partial A_0} \\ \vdots & \ddots & \vdots \\ \frac{\partial A'_0}{\partial B_1} & \cdots & \frac{\partial B'_1}{\partial B_1} \end{array} \right) \bigg|_{\text{fixpoint}}. \quad (10)$$

We found that the modulus of the eigenvalues of this matrix is smaller than unity for $f_0^{\text{crit}} = 0.77184451 < f_0 \leq 1$, which means that in this interval, the fixpoint (9) is also an attractor. This is in excellent agreement with a numerical evaluation of (8), where we found that $0.77182 < f_0^{\text{crit}} < 0.77188$.

We also evaluated (8) numerically in order to investigate correlated noise (see Fig. 2). Like in the case of uncorrelated noise, we found that the coefficients A_0 and B_1 reach, during the distillation process, some finite value, while the coefficients A_1 and B_0 decrease exponentially fast, whenever the noise level is moderate.

In other words, both subensembles, characterized by the value of the respective error flags, approach a pure state asymptotically. The pairs in the ensemble with error flag “0” are in the state $|\Phi^+\rangle$, while those in the ensemble with error flag “1” are in the state $|\Psi^+\rangle$.

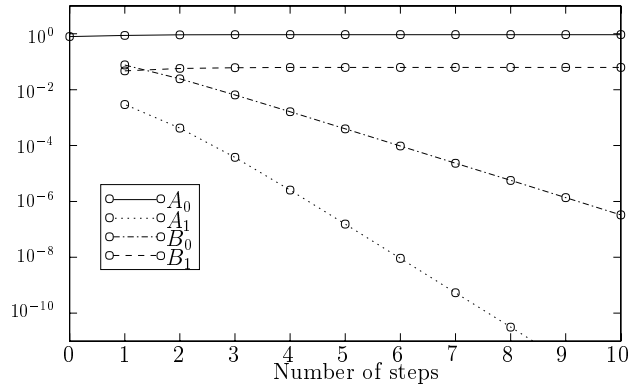


FIG. 2: The evolution of the four parameters A_0, A_1, B_0 , and B_1 . Note that both A_1 and B_0 decrease exponentially fast in the number of steps.

To conclude this section, we summarize: For a large region $0.77184451 \equiv f_0^{\text{crit}} \leq f_0 \leq 1$ the 2-EPP purifies and at the same time any eavesdropper is factored out. For a small region $0.75 < f_0 < f_0^{\text{crit}} \equiv 0.77184451$, close to the threshold of the purification protocol, the conditional fidelity does not reach unity, while the protocol is in the purification regime. Even though the region is small and of little practical relevance (in this regime we are already

out of the repeater regime [13] and purification is very inefficient), its existence shows that the process of factorization is an independent phenomenon and not trivially connected to EPP. A more exhaustive description of the intermediate regime will be published elsewhere.

C. Bell diagonal initial states

Now we want to show that the same result is true for arbitrary Bell diagonal states (Eq. (1)) and for noise of the form (4). The procedure is the same as in the case of binary pairs; however, a few modifications are required.

In order to keep track of the four different error operators σ_μ in (4), the lab demon has to attach two classical bits to each pair; let us call them the phase error bit and amplitude error bit. Whenever a σ_x (σ_z , σ_y) error occurs, the lab demon inverts the error amplitude bit (error phase bit, both error bits). To update these error flags, he uses the update function given in Tab. I). The physical reason for the choice of the flag update function will be given in the next section.

	(00)	(01)	(10)	(11)
(00)	(00)	(00)	(00)	(10)
(01)	(00)	(01)	(11)	(00)
(10)	(00)	(11)	(01)	(00)
(11)	(10)	(00)	(00)	(00)

TABLE I: The value (phase error, amplitude error) of the updated error flag of a pair that is kept after a 2-EPP step, given as a function of the error flags of P_1 and P_2 (left to right and top to bottom, respectively).

Here, the lab demon divides all pairs into four subensembles, according to the value of their error flag. In each of the subensembles the pairs are described by a Bell diagonal density operator, like in Eq. (1), which now depends on the subensemble. That means, in order to completely specify the state of all four subensembles, there are 16 real numbers $A_{ij}, B_{ij}, C_{ij}, D_{ij}$ with $i, j \in \{0, 1\}$ required, for which one obtains recurrence relations of the form

$$\begin{aligned}
A_n^{(00)} &\rightarrow A_{n+1}^{(00)}(A_n^{(00)}, A_n^{(01)}, \dots, D_n^{(11)}), \\
A_n^{(01)} &\rightarrow A_{n+1}^{(01)}(A_n^{(00)}, A_n^{(01)}, \dots, D_n^{(11)}), \\
&\vdots \\
D_n^{(11)} &\rightarrow D_{n+1}^{(11)}(A_n^{(00)}, A_n^{(01)}, \dots, D_n^{(11)}).
\end{aligned} \tag{11}$$

These generalize the recurrence relations (8) for the case of binary pairs, and the relations (2) for the case of noiseless apparatus.

Like the recurrence relations (2) and (8), respectively, these relations are (modulo normalization) quadratic forms in the 16 state variables $\vec{a} = (A^{(00)}, A^{(00)}, \dots, D^{(11)})^T$, with coefficients that depend on the error parameters $f_{\mu\nu}$ only. In other words, (11) can be written in the more compact form

$$\vec{a}'_j = \vec{a} M_j \vec{a}^T, \tag{12}$$

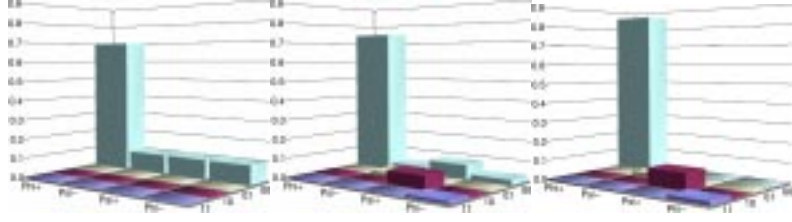


FIG. 3: The evolution of the extended state

where, for each $j \in \{1, \dots, 16\}$, M_j is a real 16×16 -matrix whose coefficients are polynomials in the noise parameters $f_{\mu\nu}$.

D. Numerical results

The 16 recurrence relations (11) imply a reduced set of 4 recurrence relations for the quantities $A_n = \sum_{ij} A_n^{(ij)}, \dots, D_n = \sum_{ij} D_n^{(ij)}$ which describe the evolution of the total ensemble (that is, the *blend* [21] of the four subensembles) under the purification protocol. Note that these values are the only ones which are known and accessible to Alice and Bob, as they have no knowledge of the values of the error flags. It has been shown in [13] that under the action of the noisy entanglement distillation process, these quantities converge towards a fixpoint $(A_\infty, B_\infty, C_\infty, D_\infty)$, where $A_\infty = F_{\max}$ is the maximal attainable fidelity [14].

Fig. 3 shows for typical initial conditions the evolution of the 16 coefficients $A_n^{(00)} \dots D_n^{(11)}$. They are organized in a 4×4 -matrix, where one direction represents the Bell state of the pair, and the other indicates the value of the error flag. The figure shows the state (a) at the beginning of the entanglement purification procedure, (b) after few purification steps, and (c) at the fixpoint. As one can see, initially all error flags are set to zero and the pairs are in a Werner state with a fidelity of 70%. After a few steps, the population of the diagonal elements starts to grow; however, none of the elements vanishes. At the fixpoint, all off-diagonal elements vanish, which means that there are *strict correlations* between the states of the pairs and their error flags.

In order to determine how fast the state converges, we investigate two important quantities: the first is the fidelity $F_n \equiv A_n$, and the second is the *conditional fidelity* $F_n^{\text{cond}} \equiv A_n^{(00)} + B_n^{(11)} + C_n^{(01)} + D_n^{(10)}$. Note that the first quantity is the sum over the four $|\Phi^+\rangle$ components in Fig. 3, while the latter is the sum over the four diagonal elements. The conditional fidelity is the fidelity which Alice and Bob would assign to the pairs if they knew the values of the error flags, i. e.

$$F_n^{\text{cond}} = \sum_{i,j} \langle \Phi^+ | \sigma_{i,j} \rho_{i,j} \sigma_{i,j} | \Phi^+ \rangle, \quad (13)$$

where $\rho_{i,j}$ is the non-normalized state of the subensemble of the pairs with the error flag (i, j) . For convenience, we used the phase- and spin-flip bits i and j as indices for the Pauli matrices, i. e. $\sigma_{00} = \text{Id}, \sigma_{01} = \sigma_x, \sigma_{11} = \sigma_y, \sigma_{10} = \sigma_z$.

The results that we obtain are similar to those for the binary pairs. We can also distinguish three regimes of noise parameters $f_{\mu\nu}$. In the high-noise regime (i. e., small values of

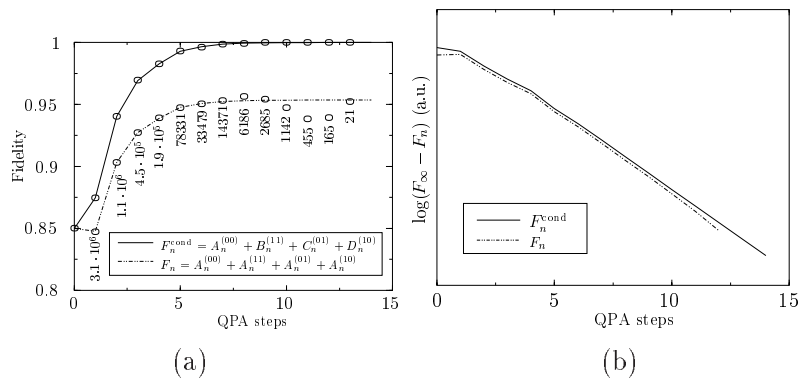


FIG. 4: (a) The fidelities F and F_{cond} as a function of the number of steps in the entanglement distillation process (analytical results (lines) and Monte Carlo simulation (circles)). For the calculation, one and two qubit white noise with a noise fidelity of 97% has been assumed. The Monte Carlo simulation was started with 10000000 pairs; the numbers indicate how many pairs are left after each step of the distillation process. This decreasing number is the reason for the increasing fluctuations around the analytical curves.

f_{00}), the noise level is above the threshold of the 2-EPP and the fidelity F and the conditional fidelity F^{cond} converge both to the value 0.25. In the low-noise regime (i.e., large values of f_{00}), F converges to the maximum fidelity F_{max} and F^{cond} converges to unity (see Fig. 4). This regime is the *security regime*, where we know that secure quantum communication is possible. Like for binary pairs, there exists also an intermediate regime, where the 2-EPP purifies but F^{cond} does not converge to unity. For an illustration, see Fig 5. Note that the size of the intermediate regime is very small, compared to the security regime. Whether or not secure quantum communication is possible in this regime is unknown. However, the answer of this question is irrelevant for all practical purposes, because in the intermediate regime the distillation process converges very slowly. A detailed discussion of the situation near the purification threshold will be published at some other place.

Even though the intermediate regime is practically irrelevant, it is important to estimate its size. For simplicity, we considered the case of one-qubit white noise, i.e. $f_{\mu\nu} = f_\mu f_\nu$ and $f_1 = f_2 = f_3 = (1 - f_0)/3$. Here, this regime is known to be bounded by

$$0.8983 < f^{\text{crit,lower}} < f_0 < f^{\text{crit,upper}} < 0.8988.$$

Regarding the efficiency of the distillation process, it is an important question how many initial pairs are needed to create one pair with the *security parameter* $\epsilon \equiv 1 - F^{\text{cond}}$. Both the number of required initial pairs (resources) and the security parameter scale exponentially with the number of distillation steps, so that we expect a polynomial relation between the resources and the security parameter ϵ . Fig. 6 shows this relation in a log-log plot for different noise parameters. The straight lines are fitted polynomial relations; the fit region is indicated by the lines themselves.

IV. DISCUSSION

We have shown in the preceding section, that the two-way entanglement distillation process is able to disentangle any eavesdropper from Bell pairs distributed between Alice

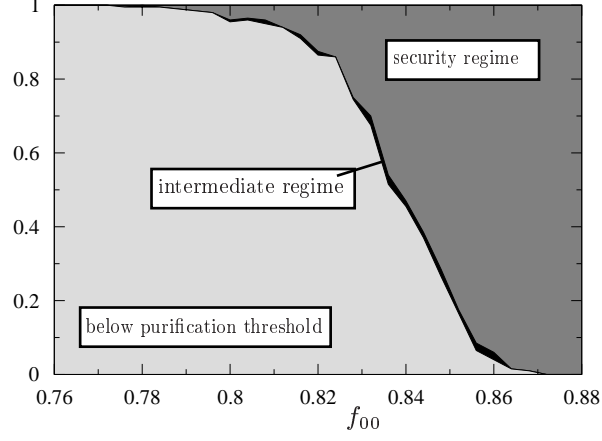


FIG. 5: The size and the location of the three regimes of the distillation process. For fixed values of f_{00} , the remaining 15 noise parameters $f_{\mu\nu}$ have been chosen at random. Plotted is the relative frequency of finding the noise parameters in any of the three regimes as a function of f_{00} .

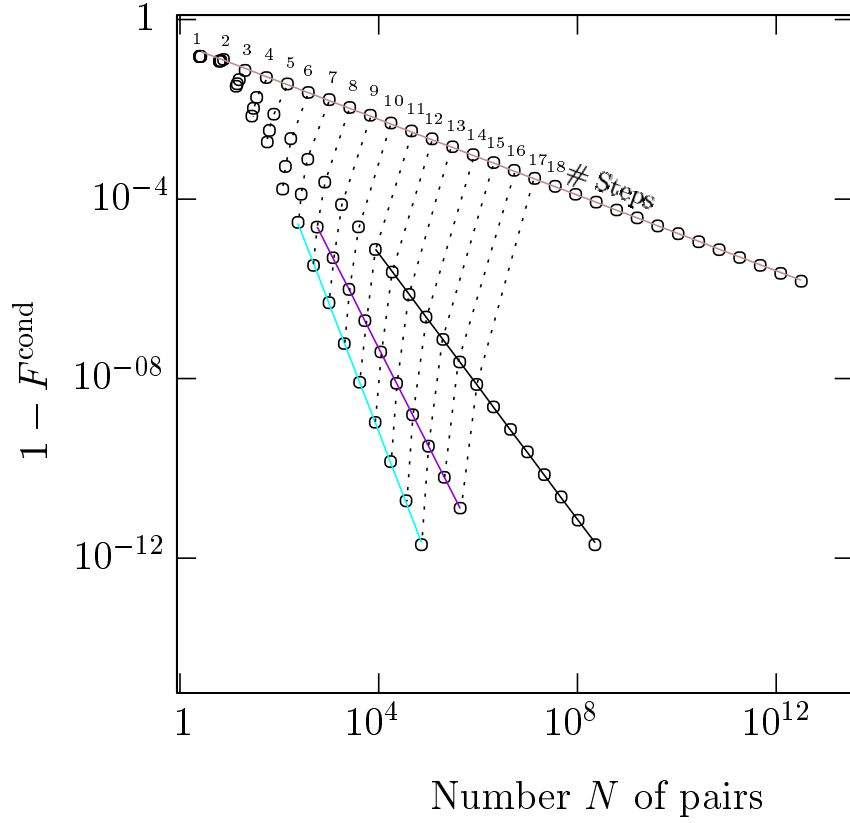


FIG. 6: Number N of pairs needed to create one pair with conditional fidelity F^{cond} . The initial state of the pairs was of the Werner type with fidelity $F_0 = 85\%$. One- and two-qubit errors were assumed with noise parameters $f_{1\text{bit}} = f_{2\text{bit}} = 0.95, 0.98, 0.99, 0.995$ (from top to bottom).

and Bob, even in the presence of noise, i.e. when the pairs can only be purified up to a specific maximum fidelity $F_{\max} < 1$. Alice and Bob may use them as a secure quantum communication channel. They are thus able to perform secure quantum communication, and, as a special case, secure classical communication (which is in this case equivalent to a key distribution scheme).

In order to keep the argument transparent, we first considered the case where noise of the form (4) is explicitly introduced by a fictitious lab-demon, who keeps track of all error operations and performs calculations. However, using a simple indistinguishability argument (see Section III A), we could show that any apparatus with the noise characteristics (4) is equally secure as a situation where noise is introduced by the lab demon. This means that the security of the protocol does not depend on the fact whether or not anybody actually calculates the flag update function. It is sufficient to just use a noisy 2-EPP, in order to get a secure quantum channel.

For the proof, we had to make several assumptions on the noise that acts in Alice's and Bob's entanglement purification device. One restriction is that we only considered noise which is of the form (4). However, this restriction is only due to technical reasons; we conjecture that our results are also true for most general noise models of the form (3). We have also implicitly introduced the assumption that the eavesdropper has no additional knowledge about the noise process, i.e. Eve only knows the publicly known noise characteristics (4) of the apparatus. This assumption would not be justified, for example, if the lab demon was bribed by Eve, or if Eve was able to manipulate the apparatus in Alice's and Bob's laboratories, for example by shining in light from an optical fiber. This concern is not important from a principal point of view, as the laboratories of Alice and Bob are considered secure by assumption. On the other hand, this concern has to be taken into account in any practical implementation.

Acknowledgments

We thank C. H. Bennett, A. Ekert, G. Giedke, N. Lütkenhaus, J. Müller-Quade, R. Raußendorf, A. Schenzle, Ch. Simon and H. Weinfurter for valuable discussions. This work has been supported by the Deutsche Forschungsgemeinschaft through the Schwerpunktprogramm "Quanteninformationsverarbeitung".

-
- [1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1985), pp. 175–179.
 - [2] A. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [3] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, *Phys. Rev. Lett.* **78**, 3221 (1997).
 - [4] B. Schumacher, *Phys. Rev. A* **54**, 2614 (1996).
 - [5] D. Mayers, in *Advances in Cryptology – Proceedings of Crypto '96* (Springer-Verlag, New York, 1996), pp. 343–357, see also quant-ph/9802025.
 - [6] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in *Proceedings of the Third-Second Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2000), pp. 715–724, quant-ph/9912053.
 - [7] H. Inamori, quant-ph/0008064.

- [8] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
- [9] A. R. Calderbank and P. Shor, Phys. Rev. A **54**, 1098 (1996).
- [10] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
- [11] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [12] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
- [13] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
- [14] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).
- [15] G. Giedke, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 2641 (1999).
- [16] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
- [17] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **70**, 722 (1996).
- [18] C. Macchiavello, Phys. Lett. A **246**, 385 (1998).
- [19] H. Aschauer and H.-J. Briegel, quant-ph/0008051.
- [20] K. Kraus, *States, Effects, and Operations*, vol. 190 of *Lecture Notes in Physics* (Springer Verlag, Berlin Heidelberg New York Tokyo, 1983).
- [21] B.-G. Englert, Z. Naturforsch. **54a**, 11 (1999).